CJIS Security Policy

& the IT Security Audit

Jeff Campbell
CJIS Information Assurance Unit
(304) 625 – 4961
Jeffrey.campbell@ic.fbi.gov

Candice B. Preston
CJIS Audit Unit
(304) 625 - 2988
candice.preston@ic.fbi.gov

SHARED MANAGEMENT

Where does the criminal justice information come from?

- Local
- State
- Tribal
- Federal

Because the information is shared…

- The FBI CJIS Division employs a shared management philosophy

What does 'shared management' mean?

- The FBI along with local, state, tribal, and federal data providers and system users share responsibility for the operation and management of all systems administered by the CJIS Division for the benefit of the criminal justice community.

SHARED MANAGEMENT

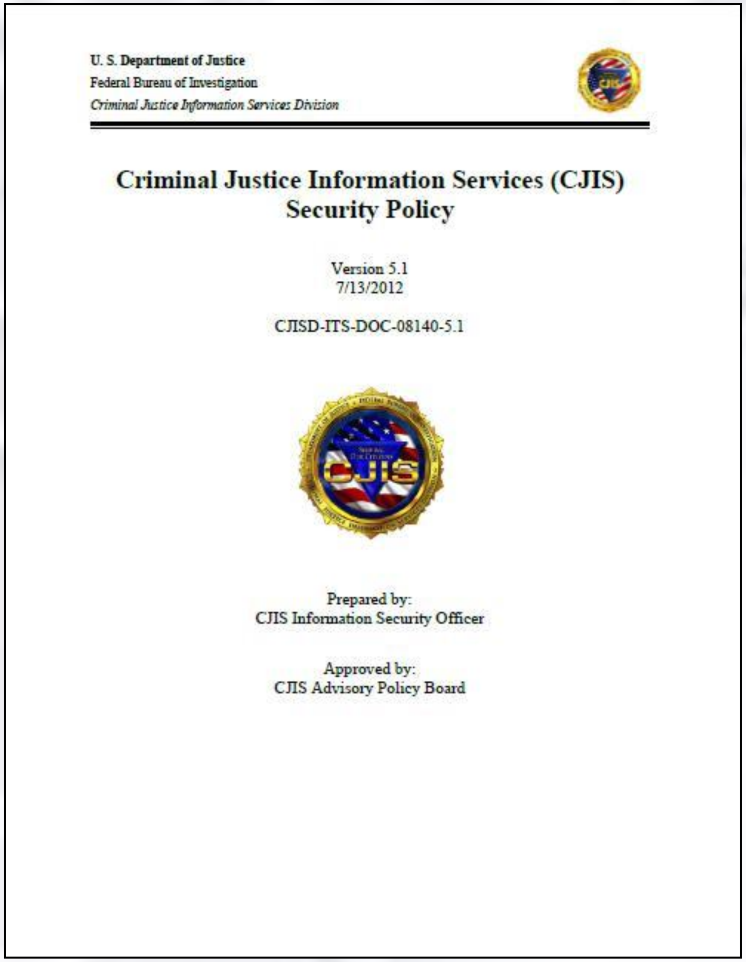
How does ‘shared management’ work?

- Designation of a CJIS Systems Agency (CSA)
- Designation of a CJIS Systems Officer (CSO)
- CJIS Advisory Process

The CJIS Advisory Process is used to…

- obtain the user community’s advice and guidance on the operation of all of the CJIS programs
- establish a minimum standard of requirements to ensure continuity of information protection (write minimum policy standards)
- represent the shared responsibility between the FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI

CJIS SECURITY POLICY OVERVIEW



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS)
Security Policy

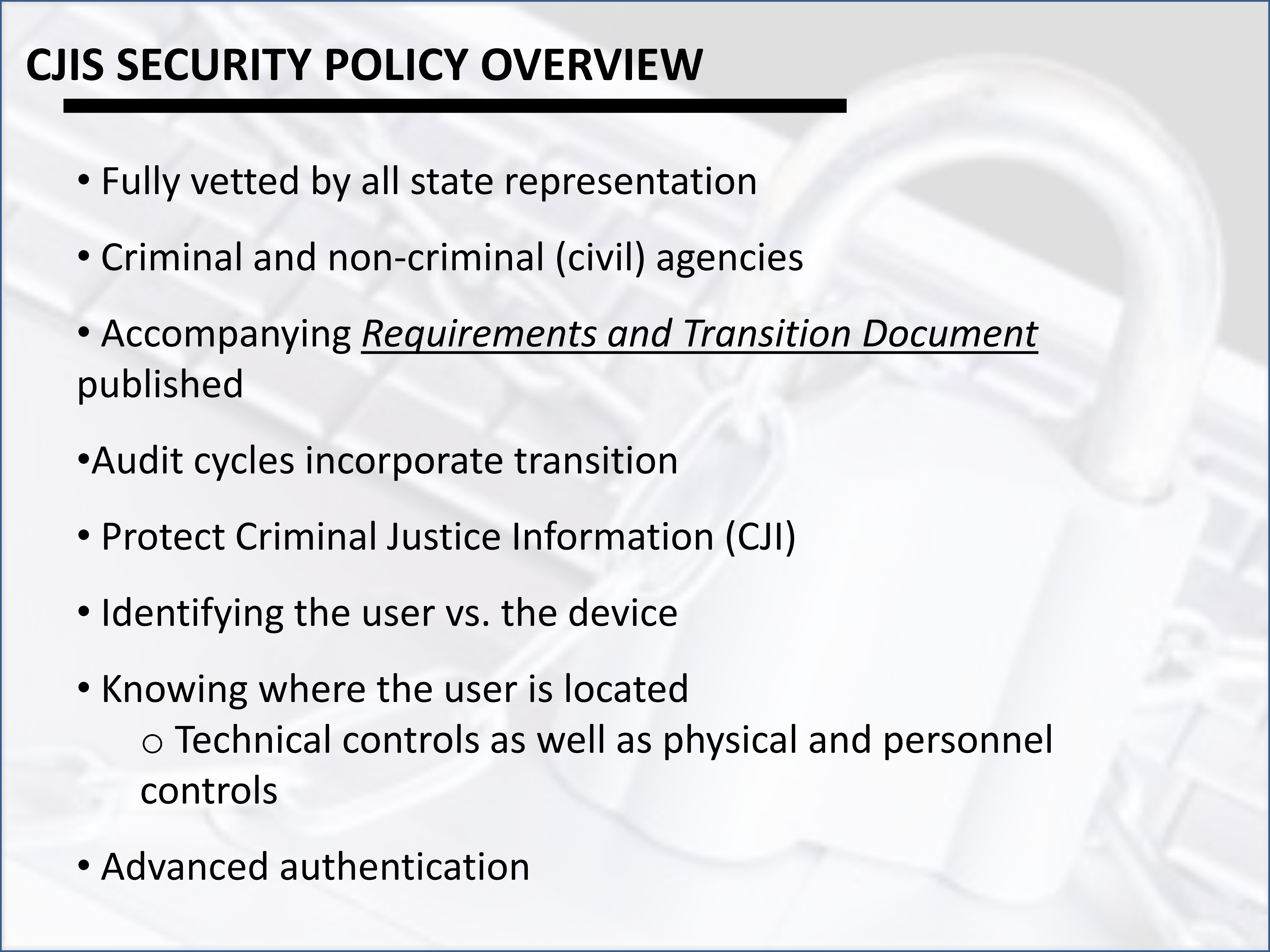
Version 5.1
7/13/2012

CJISD-ITS-DOC-08140-5.1

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

Presented by: Jeff Campbell, FBI CJIS Assistant ISO



CJIS SECURITY POLICY OVERVIEW

- Fully vetted by all state representation
- Criminal and non-criminal (civil) agencies
- Accompanying *Requirements and Transition Document* published
- Audit cycles incorporate transition
- Protect Criminal Justice Information (CJI)
- Identifying the user vs. the device
- Knowing where the user is located
    - Technical controls as well as physical and personnel controls
- Advanced authentication

CJIS SECURITY POLICY OVERVIEW

Sections 1 – 4

Introduces the CJIS Security Policy, describes the approach used throughout the document, and defines roles and responsibilities

- Community of Criminal Justice Information (CJI)
  - State, county, local, territory, tribe, federal, international criminal justice AND non-criminal justice
  - Private industry

- CJI extends the protection measures of information beyond CHRI to include PII

CJIS SECURITY POLICY OVERVIEW

Section 5

Policy Areas 1 - 12

- Focus on the data and services that the FBI CJIS Division exchanges and provides.

- Strategic reasoning and tactical implementation requirements and standards.

- Further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges.

- Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life cycle.

CJIS SECURITY POLICY OVERVIEW

Section 5

Policy Areas 1 - 12

Policy Area 1—Information Exchange Agreements

Policy Area 2—Security Awareness Training

Policy Area 3—Incident Response

Policy Area 4—Auditing and Accountability

Policy Area 5—Access Control

Policy Area 6—Identification and Authentication

CJIS SECURITY POLICY OVERVIEW

Section 5

Policy Areas 1 - 12

Policy Area 7—Configuration Management

Policy Area 8—Media Protection

Policy Area 9—Physical Protection

Policy Area 10—Systems and Communications Protection and Information Integrity

Policy Area 11—Formal Audits

Policy Area 12—Personnel Security

Appendices

Appendix A —Terms and Definitions

Appendix B —Acronyms

Appendix C —Network Topology Diagrams

Appendix D —Sample Information Exchange Agreements

Appendix E —Security Forms and Organizational Entities

Appendix F —IT Security Incident Response Form

Appendix G —Best Practices

Appendix H —Security Addendum

Appendix I —References

Appendix J —Noncriminal Justice Agency Supplemental Guidance

Appendix K —Criminal Justice Agency Supplemental Guidance

CJIS SECURITY POLICY OVERVIEW

Significant Changes in v5.2

Section 4.1 Definition of CJI

Section 5.1.1 Policy to validate requestor as authorized user

Section 5.2 Realignment of training requirements

Section 5.9.1.8 Visitor Log

Several mobile device changes

Advanced Authentication exemption expiration dates

Best practices appendix additions

CJIS AUDIT UNIT

Why does the FBI audit?

- Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies
- Information housed in CJIS systems is obtained from the user community; the audit ensures that all agencies with access protect the data of the community at large

What does the audit accomplish?

- Assists agencies with compliance
- Verifies adherence to policy and procedure
- Evaluates agency practices and procedures and their effectiveness
- Improves and ensures the integrity of the system data
- Protects and safeguards criminal justice information (CJI)
- Protects continuity of information
- Limits agency liability
- Improves officer safety and public safety

CJIS AUDIT UNIT

Who does the FBI audit?

- Each CJIS Systems Agency (CSA), every 3 years

If the audit is of the CSA, why do local agencies participate?

- In order to assess each state’s overall compliance, the FBI CJIS Audit Unit (CAU) selects a number of local law enforcement agencies throughout the state to participate in the audit of their CSA

- If your local agency has been selected to participate, it is only because the agency accepts access to criminal justice information (CJI) through your state CSA

I received an audit from my CSA, is this the same?

- No, much like the APB requires the FBI to audit each CSA, each CSA must audit all criminal justice agencies (CJAs) with access to CJIS systems within their state. Although content will be similar, the audit is not the same.

CJIS AUDIT UNIT

If my local agency is chosen, what can I expect?

- Initial call from the FBI Auditor (contact information for this call is provided by the CSA)

- Official written notice is sent to the Head of the Agency (Chief or Sheriff)

- Pre-audit material forwarded electronically to audit point of contact
  - Provides general idea of topic areas that will be discussed
  - List of documentation the agency is required to provide
  - Provides an idea of who to have present during the audit

- Onsite audit includes an administrative interview conducted with appropriate agency personnel. Following the interview, the auditor may perform a physical security inspection, which involves a tour of the facility, including anywhere the agency is processing, storing, or accessing CJI

- Agency documentation is reviewed

- At the conclusion of the audit, the agency will receive a policy assessment packet. The packet summarizes those policy requirements assessed during the audit, but the packet also provides the agency’s compliance status. Any concerns or compliance issues found will be discussed with appropriate agency personnel at the time of the audit.

CJIS AUDIT UNIT

What happens following the local audit?

- All local agency audit findings are compiled into a draft report and provided to the CSA roughly 60 days following the onsite audit

- The CSA is then given 30 days to respond with corrective action plans for each local agency that participated in their audit

- The CSA will work with each local agency on a strategy to bring that agency into compliance

- The APB's Compliance Evaluation Subcommittee reviews the audit results and the corresponding responses to determine the course of action necessary to bring agencies into compliance

- The APB's Compliance Evaluation Subcommittee routinely considers long-term strategies, sometimes over several budget cycles, when approving plans for corrective action

CJIS AUDIT UNIT

What are the most common ITSA findings?

- Authentication (passwords)
- Security Awareness Training
- Information Exchange Agreements [Management Control Agreements (NCJA) / Security Addendums (private contractors)]
- Personnel Security (fingerprint based record checks)
- Encryption

CJIS AUDIT UNIT

What were the audit findings of the 2010 MSP audit?

- Information Exchange Agreements [Management Control Agreements (NCJA) / Security Addendums (private contractors)]\
- Management Control of networks that transmit CJI
- Personnel Security (fingerprint based record checks)
- Security Awareness Training
- Media Protection/Destruction (written policy)
- Authentication (passwords)
- Advanced Authentication
- Encryption

CJIS SECURITY POLICY

Section 3

Roles and Responsibilities

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

CJIS SECURITY POLICY

Section 5.2

Policy Area 2: Security Awareness Training

Requirements:

- Within six (6) months of initial assignment
- Biennially

Three “Levels” of topics:

1. All Personnel
2. Personnel with Physical and Logical Access
3. Personnel with Technology Roles

Training Records:

- Documented
- Kept current
- Maintained by CSO/SIB/Compact Council

Section 5.6
Policy Area 6: Identification and Authentication

What is authentication?

- The process of verifying a claimed identity
- Determining if the subject is really who he/she claims to be

Based on at least one of the following three factors:

- Something a person knows (password, passphrase, PIN)
- Something a person has (smart card, token, key, swipe card, badge)
- Something a person is (fingerprint, voice, retina/iris characteristics)

Strong, or two-factor, authentication contains two (distinct) out of three of these methods.

Section 5.6
Policy Area 6: Identification and Authentication

What is advanced authentication (AA)?

- The process of requiring more than a single factor of authentication

When is AA required?

- “Dependent upon the physical, personnel, and technical security controls associated with the user location.” (Section 5.6.2.2.1)
    - o When outside a physically secure location
    - o When inside a physically secure location (Section 5.9) where the technical controls (Section 5.5 and 5.10) have not been implemented
    - o At the point of CJI access

CJIS SECURITY POLICY

Section 5.6
Policy Area 6: Identification and Authentication

Are there exceptions or exemptions to requiring AA?

- Section 5.6.2.2.1 – Interim Compliance
    - Accessing CJI from devices associated with, and located
    - within a police vehicle are exempt
        - Unless procured/upgraded since 2005
    - IPSec
        - Funded prior to 2011
        - For purpose of AA

Currently expires: September 30, 2014

Section 5.7.1.2
Network Diagram

Why do we need a network diagram?

- Based on NIST SP 800-53 controls

Requirements

- System interconnections and data flows
- Logical location of devices
- Agency name and date of diagram
- Classification markings

Samples in Appendix C

CJIS SECURITY POLICY

Section 5.10.1.2

Encryption

When encryption is used, it must be FIPS 140-2 certified

- Based on NIST SP 800-53 controls

Criminal Justice Information (CJI) must be encrypted:

- When stored (at rest) outside the boundary of a physically secure location
- Immediately when transmitted outside the boundary of a physically secure location (two exceptions: 5.5.7.3.2 and 5.10.2)

Mobile Devices

MDTs/Laptops

- Large form factor
- Full featured OS

Tablets

- Medium form factor
- Limited feature OS

Smartphones

- Small form factor
- Limited feature OS

CJIS SECURITY POLICY

Mobile Devices

Where are we now?

- Current requirements: 5.5.7, 5.10.4.2, 5.10.4.3, 5.10.4.4
- Mobile Device Management (MDM): NEW! 5.5.7.3.3

Where are we going?

- A dedicated policy area (5.13)
- Additional requirements specific to non-traditional mobile devices

CJIS SECURITY POLICY

Firewalls

5.10.1.1 Boundary Protection

- 3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).

5.10.4.4 Personal Firewall

- A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy.

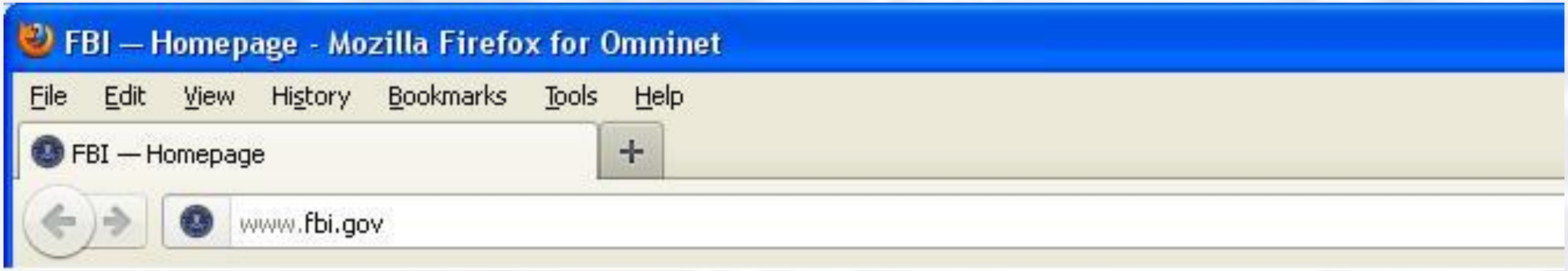
5.5.7.3.1 Cellular Risk Mitigation

- Employ personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services from the agency level.

CJIS SECURITY POLICY RESOURCE CENTER

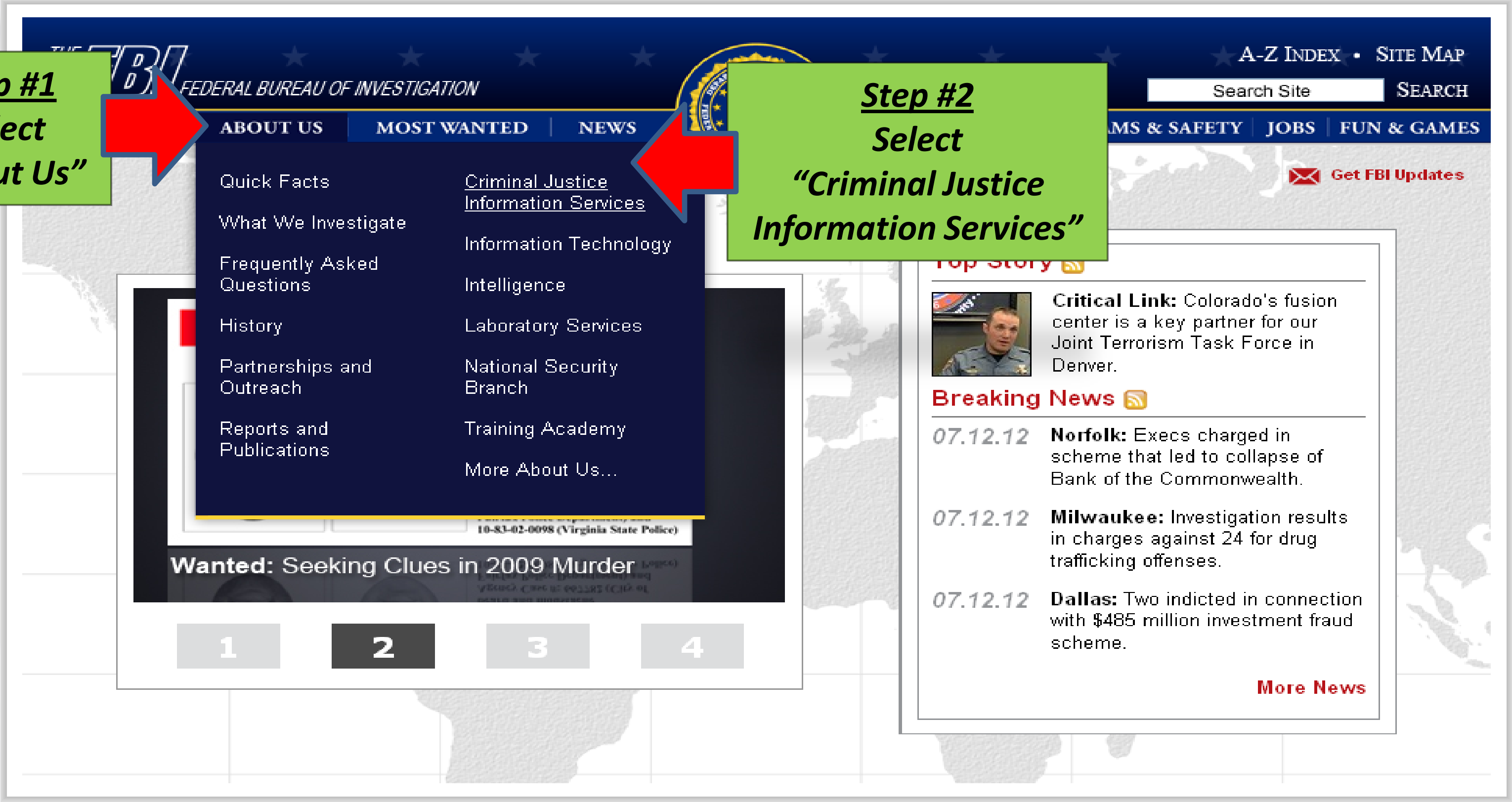
Now, the CJIS Security Policy can be experienced online through the fbi.gov web portal!

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view



CJIS SECURITY POLICY RESOURCE CENTER

Now, the CJIS Security Policy can be experienced online through the fbi.gov web portal! Once arriving at fbi.gov, select the "ABOUT US" category, then select the link for Criminal Justice Information Services link as depicted below:



Step #1
Select "About Us"

Step #2
Select "Criminal Justice Information Services"

Wanted: Seeking Clues in 2009 Murder

Critical Link: Colorado's fusion center is a key partner for our Joint Terrorism Task Force in Denver.

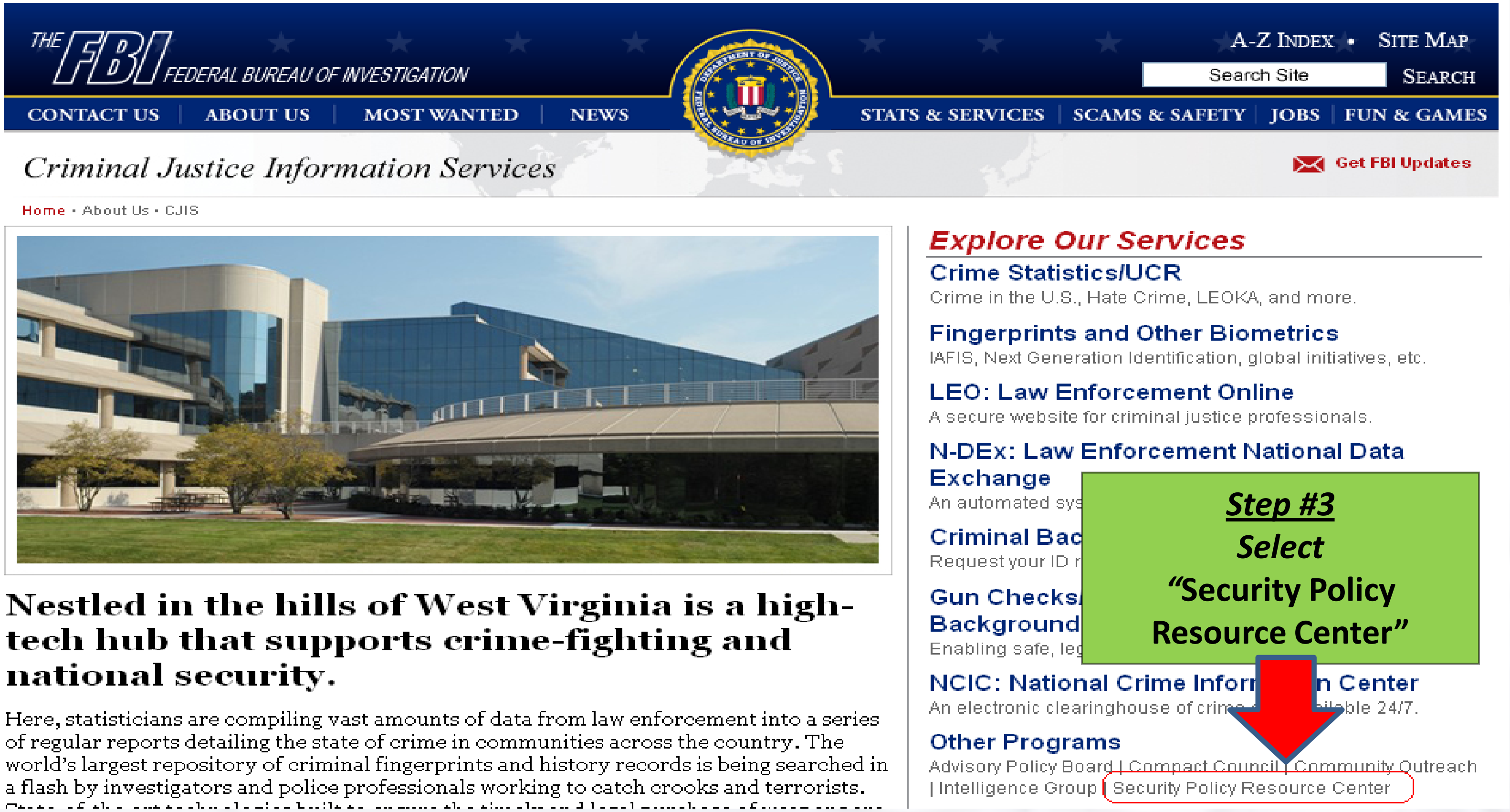
07.12.12 **Norfolk:** Execs charged in scheme that led to collapse of Bank of the Commonwealth.

07.12.12 **Milwaukee:** Investigation results in charges against 24 for drug trafficking offenses.

07.12.12 **Dallas:** Two indicted in connection with $485 million investment fraud scheme.

CJIS SECURITY POLICY RESOURCE CENTER

Once arriving at the CJIS page, select the link entitled "Security Policy Resource Center" as depicted below:



Criminal Justice Information Services

Nestled in the hills of West Virginia is a high-tech hub that supports crime-fighting and national security.

Here, statisticians are compiling vast amounts of data from law enforcement into a series of regular reports detailing the state of crime in communities across the country. The world's largest repository of criminal fingerprints and history records is being searched in a flash by investigators and police professionals working to catch crooks and terrorists.

Explore Our Services

Crime Statistics/UCR
Crime in the U.S., Hate Crime, LEOKA, and more.

Fingerprints and Other Biometrics
IAFIS, Next Generation Identification, global initiatives, etc.

LEO: Law Enforcement Online
A secure website for criminal justice professionals.

N-DEx: Law Enforcement National Data Exchange
An automated sys

Criminal Bac
Request your ID r

Gun Checks/ Background
Enabling safe, leg

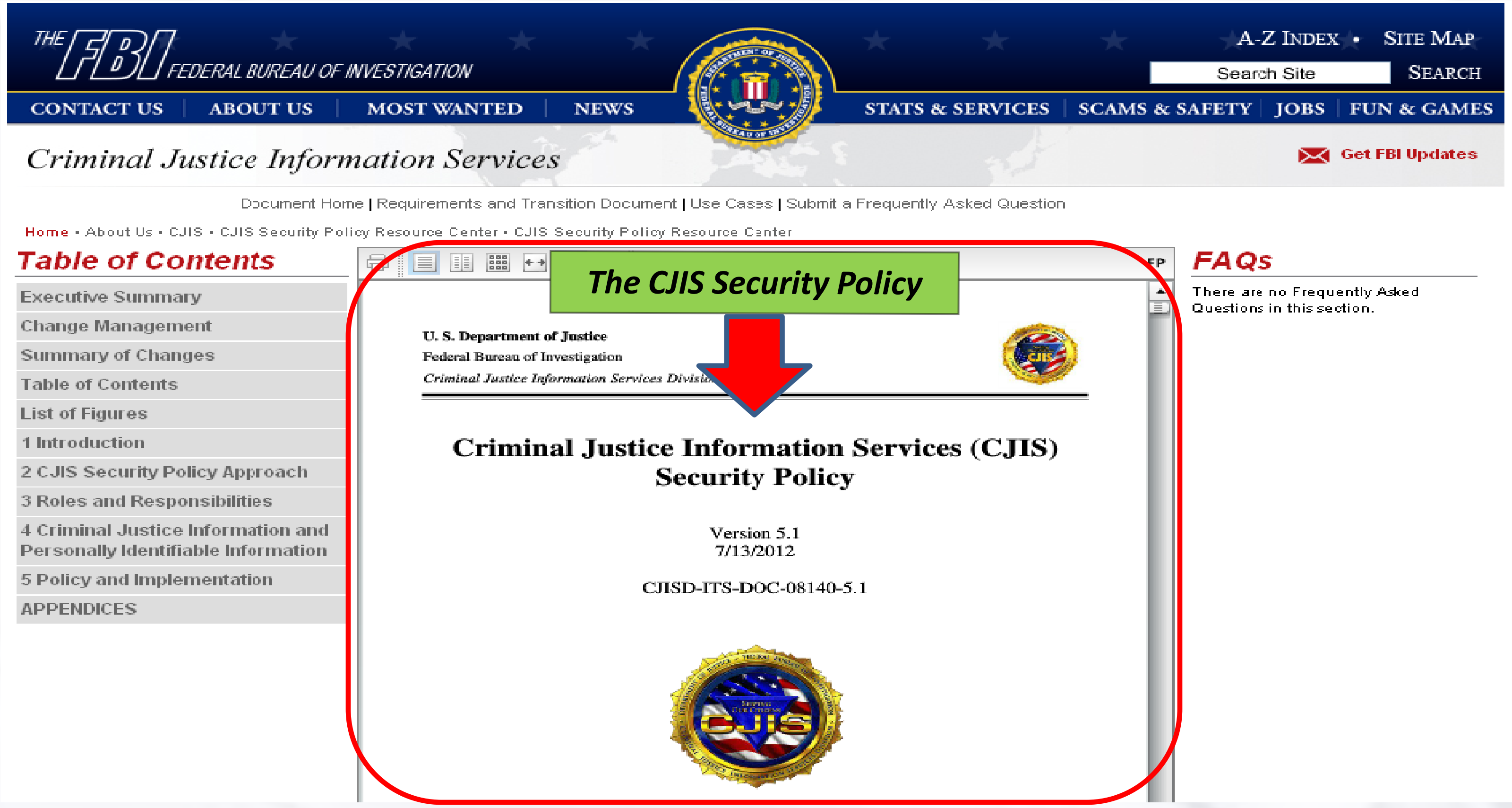
NCIC: National Crime Infor n Center
An electronic clearinghouse of crim ilable 24/7.

Other Programs
Advisory Policy Board | Compact Council | Community Outreach | Intelligence Group | Security Policy Resource Center

Step #3
Select
"Security Policy Resource Center"

CJIS SECURITY POLICY RESOURCE CENTER

After selecting the link “CJIS Security Policy Resource Center” you will be directed to the page shown below which contains the CJIS Security Policy AND some additional features and resources.



THE FBI FEDERAL BUREAU OF INVESTIGATION
A-Z INDEX • SITE MAP
Search Site
SEARCH
CONTACT US | ABOUT US | MOST WANTED | NEWS
STATS & SERVICES | SCAMS & SAFETY | JOBS | FUN & GAMES
Get FBI Updates

Criminal Justice Information Services

Document Home | Requirements and Transition Document | Use Cases | Submit a Frequently Asked Question

Home • About Us • CJIS • CJIS Security Policy Resource Center • CJIS Security Policy Resource Center

Table of Contents

The CJIS Security Policy

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.1
7/13/2012

CJISD-ITS-DOC-08140-5.1

FAQs

There are no Frequently Asked Questions in this section.

QUESTIONS

Jeff Campbell

CJIS Information Assurance Unit

(304) 625 - 4961

jeffrey.campbell@ic.fbi.gov

iso@leo.gov

Candice Preston

CJIS Audit Unit

(304) 625 - 5557

candice.preston@ic.fbi.gov

CJIS AUDIT UNIT CONTACT INFORMATION

NCIC AUDITS:	**Shellie Williams** shellie.williams@leo.gov	**(304) 625–2621**
IAFIS AUDITS:	**Timothy Neal** timothy.neal@ic.fbi.gov	**(304) 625 – 2637**
N-DEx AUDITS:	**Susan Gilbert-Kiger** kiger@ic.fbi.gov	**(304) 625 – 2788**
IT SECURITY AUDITS:	**Chris Wright – CJ Audits** christopher.e.wright@leo.gov	**(304) 625–2933**
	Derek Holbert – Special Audits derek.holbert@leo.gov	**(304) 625–5479**
UCR / QAR AUDITS:	**Joyce Humphrey** joyce.humphrey@leo.gov	**(304) 625–2920**
NICS AUDITS:	**Randall Wickline** randall.wickline@leo.gov	**(304) 625–4876**

CJIS ISO CONTACT INFORMATION

George A. White, CJIS ISO george.white@ic.fbi.gov	**(304) 625 - 5849**
Jeffrey B. Campbell, CJIS Assistant ISO jeffrey.campbell@ic.fbi.gov	**(304) 625 – 4961**
Stephen C. Exley, Sr. Technical Analyst stephen.exley@leo.gov	**(304) 625 - 2670**

iso@leo.gov